

**APPENDIX SHOWING DIFFERENCES BETWEEN THE CLAIMS OF THE PRESENT
APPLICATION AND THE CLAIMS OF PARENT APPLICATION 09/366,210**

1 1. A method for establishing state information for a call between a calling party and
2 a called party, comprising:

3 receiving, at an originating gate controller, a setup request for a call, the originating gate
4 controller being connected to a ~~first~~trusted network, the calling party being associated with an
5 originating interface unit coupled to a ~~second~~an untrusted network that is different from said
6 ~~first~~trusted network;

7 authorizing the setup request for the call;

8 sending the authorized setup request to the called party;

9 formatting state information for the call based on a setup acknowledgment message
10 received from the called party; and

11 sending the state information for the call from the originating gate controller to the
12 originating interface unit without maintaining the state information at the originating gate
13 controller,

14 said originating gate controller and said originating interface unit communicating with
15 one another via ~~an~~a telecommunications access network.

1 2. The method of claim 1, further comprising:

2 encrypting, at the originating gate controller, the state information for the call before
3 sending the state information from the originating gate controller to the originating interface unit,
4 the state information being sent to the originating interface unit being in encrypted form.

1 3. The method of claim 1, further comprising:

2 performing, at the originating gate controller, a cryptographic hash function on the state
3 information to produce a hash-value; and

4 sending the hash value from the originating gate controller to the originating interface
5 unit.

4. The method of claim 1, further comprising: encrypting, at the originating gate controller, the state information for the call before sending the state information from the originating gate controller to the originating interface unit, the state information being sent to the originating interface unit being in encrypted form;

performing, at the originating gate controller, a cryptographic hash function on the state information to produce a hash-value; and

sending the hash value from the originating gate controller to the originating interface unit.

5. A method for establishing state information for a call between a calling party and a called party, comprising:

receiving, at an originating gate controller, a setup request for a call, the originating gate controller being connected to a ~~first~~trusted network, the calling party being associated with an originating interface unit coupled to a ~~second~~an untrusted network;

authorizing the setup request for the call;

sending the authorized setup request to the called party;

formatting state information for the call based on a setup acknowledgment message received from the called party;

sending the state information for the call from the originating gate controller to the originating interface unit without maintaining the state information at the originating gate controller;

receiving a call feature request for the call at the originating gate controller;

receiving the state information at the originating gate controller from the originating interface unit;

modifying the state information based on the call feature request; and

sending the modified state information for the call from the originating gate controller to the originating interface unit without maintaining the modified state information at the originating gate controller.

6. A computer-readable medium having stored thereon instructions for establishing state information for a call between a calling party and a called party, the instructions when executed by a processor cause the processor to:

receive, at an originating gate controller, a setup request for a call, the originating gate controller being connected to a ~~first~~trusted network, the calling party being associated with an originating interface unit coupled to ~~a second~~an untrusted network that is different from said ~~first~~trusted network;

authorize the setup request for the call;

send the authorized setup request to the called party;

format state information for the call based on a setup acknowledgment message received from the called party; and

send the state information for the call from the originating gate controller to the originating interface unit without maintaining the state information at the originating gate controller,

said originating gate controller and said originating interface unit communicating with one another via ~~an~~access telecommunications access network.

7. The computer-readable medium of claim 6, having stored thereon instructions that when executed by the processor further cause the processor to:

encrypt, at the originating gate controller, the state information for the call before sending the state information from the originating gate controller to the originating interface unit, the state information being sent to the originating interface unit being in encrypted form.

8. The computer-readable medium of claim 6, having stored thereon instructions that when executed by the processor further cause the processor to:

perform, at the originating gate controller, a cryptographic hash function on the state information to produce a hash value; and

send the hash value from the originating gate controller to the originating interface unit.

9. The computer-readable medium of claim 6, having stored thereon instructions that when executed by the processor further cause the processor to:

3 encrypt, at the originating gate controller, the state information for the call before sending
 4 the state information from the originating gate controller to the originating interface unit, the
 5 state information being sent to the originating interface unit being in encrypted form;
 6 perform, at the originating gate controller, a cryptographic hash function on the state
 7 information to produce a hash value; and
 8 send the hash value from the originating gate controller to the originating interface unit.

1 10. A computer-readable medium having stored thereon instructions for establishing
 2 state information for a call between a calling party and a called party, the instructions when
 3 executed by a processor cause the processor to:
 4 receive, at an originating gate controller, a setup request for a call, the originating gate
 5 controller being connected to a ~~first~~trusted network, the calling party being associated with an
 6 originating interface unit coupled to a ~~second~~an untrusted network;
 7 authorize the setup request for the call;
 8 send the authorized setup request to the called party;
 9 format state information for the call based on a setup acknowledgment message received
 10 from the called party;
 11 send the state information for the call from the originating gate controller to the
 12 originating interface unit without maintaining the state information at the originating gate
 13 controller;
 14 receive a call feature request for the call at the originating gate controller;
 15 receive the state information at the originating gate controller from the originating
 16 interface unit;
 17 modify the state information based on the call feature request; and
 18 send the modified state information for the call from the originating gate controller to the
 19 originating interface unit without maintaining the modified state information at the originating
 20 gate controller.

1 11. A method for establishing state information for a call between a calling party and
 2 a called party, comprising:

receiving, at a terminating gate controller, a setup request for a call, the terminating gate controller being connected to a ~~first~~trusted network, the called party being associated with a terminating interface unit coupled to a ~~second~~an untrusted network that is different from said ~~first~~trusted network, the setup request being authorized for the call;

formatting state information for the call based on the setup request for the call; and
sending the state information for the call from the terminating gate controller to the terminating interface unit without maintaining the state information at the terminating gate controller;

said terminating gate controller and said terminating interface unit communicating with one another via ~~an~~telecommunications access network.

12. The method of claim 11, further comprising:
encrypting, at the terminating gate controller, the state information for the call before sending the state information from the terminating gate controller to the terminating interface unit,
the state information being sent to the terminating interface unit being in encrypted form.

13. The method of claim 11, wherein:
performing, at the terminating gate controller, a cryptographic hash value on the state information to produce a hash value; and
sending the hash value from the terminating gate controller to the terminating interface unit.

14. The method of claim 11, further comprising:
encrypting, at the terminating gate controller, the state information for the call before sending the state information from the terminating gate controller to the terminating interface unit, the state information being sent to the terminating interface unit being in encrypted form;
performing, at the terminating gate controller, a cryptographic hash value on the state information to produce a hash value; and
sending the hash value from the terminating gate controller to the terminating interface unit.

1 15. A method for establishing state information for a call between a calling party and
2 a called party, comprising:

3 receiving, at a terminating gate controller, a setup request for a call, the terminating gate
4 controller being connected to a ~~first~~trusted network, the called party being associated with a
5 terminating interface unit coupled to a ~~second~~untrusted network, the setup request being
6 authorized for the call;

7 formatting state information for the call based on the setup request for the call;

8 sending the state information for the call from the terminating gate controller to the
9 terminating interface unit without maintaining the state information at the terminating gate
10 controller;

11
12 receiving a call feature request for the call at the terminating gate controller;

13 receiving the state information at the terminating gate controller from the terminating
14 interface unit;

15 modifying the state information based on the call feature request; and

16 sending the modified state information for the call from the terminating gate controller to
17 the terminating interface unit without maintaining the modified state information at the
18 terminating gate controller.

1 16. The method of claim 11, further comprising:

2 receiving a call return request for the call at the terminating gate controller;

3 receiving the state information at the terminating gate controller from the terminating
4 interface unit, the state information having a source address associated with the calling party;

5 modifying the state information based on the call return request; and

6 sending the modified state information for the call from the terminating gate controller to
7 the terminating interface unit without maintaining the modified state information at the
8 terminating gate controller.

1 17. The method of claim 11, further comprising:

2 receiving a called-party-originated trace request for the call at the terminating gate
3 controller;

receiving the state information at the terminating gate controller from the terminating interface unit, the state information having a source address associated with the calling party; modifying the state information based on the called-party-originated trace request; and sending the modified state information for the call from the terminating gate controller to the terminating interface unit without maintaining the modified state information at the terminating gate controller.

18. A computer-readable medium having stored thereon instructions that, when executed by a processor, cause the processor to:

receive, at a terminating gate controller, a setup request for a call, the terminating gate controller being connected to a ~~first~~trusted network, the called party being associated with a terminating interface unit coupled to a ~~second~~untrusted network that is different from said ~~first~~trusted network, the setup request being authorized for the call;

format state information for the call based on the setup request for the call; and send the state information for the call from the terminating gate controller to the terminating interface unit without maintaining the state information at the terminating gate controller,

said terminating gate controller and said terminating interface unit communicating with one another via ~~an~~telecommunications access network.

19. The computer-readable medium of claim 18, having stored thereon instructions that when executed by the processor further cause the processor to:

encrypt, at the terminating gate controller, the state information for the call before sending the state information from the terminating gate controller to the terminating interface unit,

the state information being sent to the terminating interface unit being in encrypted form.

20. The computer-readable medium of claim 18, having stored thereon instructions that when executed by the processor further cause the processor to:

perform, at the terminating gate controller, a cryptographic hash function on the state information to produce a hash value; and

5 send the hash value from the terminating gate controller to the terminating interface unit.

1 21. The computer-readable medium of claim 18, having stored thereon instructions
2 that when executed by the processor further cause the processor to:

3 encrypt, at the terminating gate controller, the state information for the call before
4 sending the state information from the terminating gate controller to the terminating interface
5 unit, the state information being sent to the terminating interface unit being in encrypted form;

6 perform, at the terminating gate controller, a cryptographic hash function on the state
7 information to produce a hash value; and

8 send the hash value from the terminating gate controller to the terminating interface unit.

1 22. A computer-readable medium having stored thereon instructions that, when
2 executed by a processor, cause the processor to:

3 receive, at a terminating gate controller, a setup request for a call, the terminating gate
4 controller being connected to a ~~first~~trusted network, the called party being associated with a
5 terminating interface unit coupled to a ~~second~~untrusted network, the setup request being
6 authorized for the call;

7 format state information for the call based on the setup request for the call;

8 send the state information for the call from the terminating gate controller to the
9 terminating interface unit without maintaining the state information at the terminating gate
10 controller;

11 receive a call feature request for the call at the terminating gate controller;

12 receive the state information at the terminating gate controller from the terminating
13 interface unit;

14 modify the state information based on the call feature request; and

15 send the modified state information for the call from the terminating gate controller to the
16 terminating interface unit without maintaining the modified state information at the terminating
17 gate controller.

1 23. The computer-readable medium of claim 18, having stored thereon instructions
2 that when executed by the processor further cause the processor to:

3 receive a call return request for the call at the terminating gate controller;
 4 receive the state information at the terminating gate controller from the terminating
 5 interface unit, the state information having a source address associated with the calling party;
 6 modify the state information based on the call return request; and
 7 send the modified state information for the call from the terminating gate controller to the
 8 terminating interface unit without maintaining the modified state information at the terminating
 9 gate controller.

1 24. The computer-readable medium of claim 18, having stored thereon instructions
 2 that when executed by the processor further cause the processor to:

3 receive a called-party-originated trace request for the call at the terminating gate
 4 controller;
 5 receive the state information at the terminating gate controller from the terminating
 6 interface unit, the state information having a source address associated with the calling party;
 7 modify the state information based on the called-party-originated trace request; and
 8 send the modified state information for the call from the terminating gate controller to the
 9 terminating interface unit without maintaining the modified state information at the terminating
 10 gate controller.

1 25. A method for performing call features to a call initiated between a calling party
 2 and a called party, comprising:

3 sending the state information for the call from a gate controller to an associated interface
 4 unit without maintaining the state information at the gate controller, the gate controller being
 5 connected to a first~~trusted~~ network and the interface unit being coupled to a second~~an untrusted~~
 6 network that is different from said first~~trusted~~ network;

7 receiving a call feature request for the call at the gate controller after the state information
 8 was sent from the gate controller to the associated interface unit;

9 receiving the state information at the gate controller from the associated interface unit
 10 after the state information was sent from the gate controller to the associated interface unit;

11 modifying the state information based on the call feature request; and

12 sending the modified state information for the call from the gate controller to the
13 associated interface unit without maintaining the modified state information at the gate
14 controller,
15 said gate controller and said interface unit communicating with one another via ana
16 ~~telecommunications~~ access network.

1 26. The method of claim 25, further comprising:
2 encrypting, at the gate controller, the state information for the call before sending the
3 state information from the gate controller to the associated interface unit, the state information
4 being sent to the associated interface unit being in encrypted form; and
5 encrypting, at the gate controller, the modified state information for the call before
6 sending the modified state information from the gate controller to the associated interface unit,
7 the modified state information being sent to the associated interface unit being in encrypted
8 form.

1 27. The method of claim 25, further comprising:
2 performing, at the gate controller, a cryptographic hash function on the state information
3 to produce a first hash value;
4 sending the first hash value from the gate controller to the associated interface unit;
5 performing, at the gate controller, the cryptographic hash function on the modified state
6 information to produce a second hash value; and
7 sending the second hash value from the gate controller to the associated interface unit.

1 28. The method of claim 25, further comprising:
2 encrypting, at the gate controller, the state information for the call before sending the
3 state information from the gate controller to the associated interface unit, the state information
4 being sent to the associated interface unit being in encrypted form;
5 encrypting, at the gate controller, the modified state information for the call before
6 sending the modified state information from the gate controller to the associated interface unit,
7 the modified state information being sent to the interface unit being in encrypted form;

performing, at the gate controller, a cryptographic hash function on the state information to produce a first hash value;
 sending the first hash value from the gate controller to the associated interface unit;
 performing, at the gate controller, the cryptographic hash function on the modified state information to produce a second hash value; and
 sending the second hash value from the gate controller to the associated interface unit.

29. The method of claim 25, wherein:
 the gate controller is a terminating gate controller,
 the interface unit is a terminating interface unit associated with the called party,
 the call feature request is a call return request,
 the state information has a source address associated with the calling party, and
 a second call being connected based on the source address of the calling party.

30. The method of claim 25, wherein
 the gate controller is a terminating gate controller,
 the interface unit is a terminating interface unit associated with the called party,
 the call feature request is a called-party-originated trace request,
 the state information has a source address associated with the calling party, and
 reporting the source address of the calling party to a service provider.

31. A computer-readable medium having stored thereon instructions that, when executed by a processor, cause the processor to:
 send the state information for the call from a gate controller to an associated interface unit without maintaining the state information at the gate controller, the gate controller being connected to a first ~~trusted~~ network, the interface unit being coupled to a second ~~an untrusted~~ network;
 receive a call feature request for the call at the gate controller after the state information was sent from the gate controller to the associated interface unit;
 receive the state information at the gate controller from the associated interface unit after the state information was sent from the gate controller to the associated interface unit;

11 modify the state information based on the call feature request; and
 12 send the modified state information for the call from the gate controller to the associated
 13 interface unit without maintaining the modified state information at the gate controller.

1 32. The computer-readable medium of claim 31, having stored thereon instructions
 2 that when executed by the processor further cause the processor to:
 3 encrypt, at the gate controller, the state information for the call before sending the state
 4 information from the gate controller to the associated interface unit, the state information being
 5 sent to the associated interface unit being in encrypted form; and
 6 encrypt, at the gate controller, the modified state information for the call before sending
 7 the modified state information from the gate controller to the associated interface unit, the
 8 modified state information being sent to the associated interface unit being in encrypted form.

1 33. The computer-readable medium of claim 31, having stored thereon instructions
 2 that when executed by the processor further cause the processor to:
 3 perform, at the gate controller, a cryptographic hash function on the state information to
 4 produce a first hash value;
 5 send the first hash value from the gate controller to the associated interface unit;
 6 perform, at the gate controller, the cryptographic hash function on the modified state
 7 information to produce a second hash value; and
 8 send the second hash value from the gate controller to the associated interface unit.

1 34. The computer-readable medium of claim 31, having stored thereon instructions
 2 that when executed by the processor further cause the processor to:
 3 encrypt, at the gate controller, the state information for the call before sending the state
 4 information from the gate controller to the associated interface unit, the state information being
 5 sent to the associated interface unit being in encrypted form;
 6 encrypt, at the gate controller, the modified state information for the call before sending
 7 the modified state information from the gate controller to the associated interface unit, the
 8 modified state information being sent to the interface unit being in encrypted form;

perform, at the gate controller, a cryptographic hash function on the state information to produce a first hash value;
 send the first hash value from the gate controller to the associated interface unit;
 perform, at the gate controller, the cryptographic hash function on the modified state information to produce a second hash value; and
 send the second hash value from the gate controller to the associated interface unit.

35. The computer-readable medium of claim 31, having stored thereon instructions that when executed by the processor further cause the processor to:
 the gate controller is a terminating gate controller,
 the interface unit is a terminating interface unit associated with the called party,
 the call feature request is a call return request,
 the state information has a source address associated with the calling party, and
 a second call being connected based on the source address of the calling party.

36. The computer-readable medium of claim 31, having stored thereon instructions that when executed by the processor further cause the processor to:
 the gate controller is a terminating gate controller,
 the interface unit is a terminating interface unit associated with the called party,
 the call feature request is a called-party-originated trace request,
 the state information has a source address associated with the calling party, and
 reporting the source address of the calling party to a service provider.

37. A method for maintaining state information for a call between a calling party and a called party, comprising:
 sending a setup request for the call from an originating interface unit to an originating gate controller, the originating gate controller being connected to a ~~first~~trusted network, the originating interface unit being associated with the calling party and being coupled to a ~~second~~an untrusted network that is different from said ~~first~~trusted network; and

receiving, at the originating interface unit, state information for the call from the originating gate controller without the state information being maintained at the originating gate controller,

said originating gate controller and said originating interface unit communicating with one another via ~~ana telecommunications~~ access network.

38. The method of claim 37, wherein the received state information has been encrypted by the originating gate controller.

39. The method of claim 37, further comprising:
receiving, at the originating interface unit, a hash value from the originating gate controller,
the received hash value being based on a cryptographic hash function applied to the state information received at the originating gate controller.

40. The method of claim 37, further comprising:
receiving, at the originating interface unit, a hash value from the originating gate controller,
the received hash value being based on a cryptographic hash function applied to the state information received at the originating gate controller,
the received state information having been encrypted by the originating gate controller.

41. A method for maintaining state information for a call between a calling party and a called party, comprising:
sending a setup request for the call from an originating interface unit to an originating gate controller, the originating gate controller being connected to a ~~first~~ trusted network, the originating interface unit being associated with the calling party and being coupled to ~~a second~~ an untrusted network;
receiving, at the originating interface unit, state information for the call from the originating gate controller without the state information being maintained at the originating gate controller;

10

11 sending a call feature request for the call from the originating interface unit to the
12 originating gate controller, said call feature request including at least a portion of the state
13 information received at the originating interface unit; and

14 receiving modified state information at the originating interface unit from the originating
15 gate controller, the modified state information being based on the state information in the call
16 feature request.

1 42. A computer-readable medium having stored thereon instructions that, when
2 executed by a processor, cause the processor to:

3 send a setup request for the call from an originating interface unit to an originating gate
4 controller, the originating gate controller being connected to a ~~first~~trusted network, the
5 originating interface unit being associated with the calling party and being coupled to a ~~second~~an
6 ~~untrusted~~ network that is different from said ~~first~~trusted network, and;

7 receive, at the originating interface unit, state information for the call from the originating
8 gate controller without the state information being maintained at the originating gate controller;
9 said originating gate controller and said originating interface unit communicating with
10 one another via ~~an~~a telecommunications access network.

1 43. The computer-readable medium of claim 42, wherein the received state
2 information has been encrypted by the originating gate controller.

1 44. The computer-readable medium of claim 42, having stored thereon instructions
2 that when executed by the processor further cause the processor to::

3 receive, at the originating interface unit, a hash value from the originating gate controller,
4 the received hash value being based on a cryptographic hash function applied to the state
5 information received at the originating gate controller.

1 45. The computer-readable medium of claim 42, having stored thereon instructions
2 that when executed by the processor further cause the processor to::

3 receive, at the originating interface unit, a hash value from the originating gate controller,

the received hash value being based on a cryptographic hash function applied to the state information received at the originating gate controller,
the received state information having been encrypted by the originating gate controller.

46. A computer-readable medium having stored thereon instructions that, when executed by a processor, cause the processor to:

- send a setup request for the call from an originating interface unit to an originating gate controller, the originating gate controller being connected to a ~~first~~trusted network, the originating interface unit being associated with the calling party and being coupled to a second~~an~~ ~~untrusted~~ network;
- receive, at the originating interface unit, state information for the call from the originating gate controller without the state information being maintained at the originating gate controller;
- send a call feature request for the call from the originating interface unit to the originating gate controller, said call feature request including at least a portion of the state information received at the originating interface unit; and
- receive modified state information at the originating interface unit from the originating gate controller, the modified state information being based on the state information in the call feature request.

47. A method for maintaining state information for a call between a calling party and a called party, comprising:

- receiving an authorized setup request at a terminating interface unit from a terminating gate controller;
- sending a setup acknowledgment message based on the authorized setup request from the terminating interface unit to the terminating gate controller; and
- receiving, at the terminating interface unit, state information for the call from the terminating gate controller without the state information being maintained at the terminating gate controller;
- said terminating interface unit and said terminating gate controller communicating over ~~ana telecommunications~~ access network.

1 48. The method of claim 47, wherein the received state information has been
2 encrypted by the terminating gate controller.

1 49. The method of claim 47, further comprising:
2 receiving, at the terminating interface unit, a hash value from the terminating gate
3 controller,
4 the received hash value being based on a cryptographic hash function being applied on
5 the state information received at the terminating gate controller.

1 50. The method of claim 47, further comprising:
2 receiving, at the terminating interface unit, a hash value from the terminating gate
3 controller,
4 the received hash value being based on a cryptographic value being applied on the state
5 information received at the terminating gate controller,
6 the received state information has been encrypted by the terminating gate controller.

1 51. The method of claim 50 wherein

1 52. A computer-readable medium having stored thereon instructions that, when
2 executed by a processor, cause the processor to:
3 receive an authorized setup request at a terminating interface unit from a terminating gate
4 controller;
5 send a setup acknowledgment message based on the authorized setup request from the
6 terminating interface unit to the terminating gate controller;
7 receive, at the terminating interface unit, state information for the call from the
8 terminating gate controller without the state information being maintained at the terminating gate
9 controller;
10 said terminating interface unit and said terminating gate controller communicating over
11 ana telecommunications access network.

53. The computer-readable medium of claim 52, wherein the received state information has been encrypted by the terminating gate controller.

54. The computer-readable medium of claim 52, having stored thereon instructions that when executed by the processor further cause the processor to::
receive, at the terminating interface unit, a hash value from the terminating gate controller,
the received hash value being based on a cryptographic hash function being applied on the state information received at the terminating gate controller.

55. The computer-readable medium of claim 52, having stored thereon instructions that when executed by the processor further cause the processor to::
receive, at the terminating interface unit, a hash value from the terminating gate controller,
the received hash value being based on a cryptographic hash function being applied on the state information received at the terminating gate controller,
the received state information has been encrypted by the terminating gate controller.

56. The computer-readable medium of claim 52 wherein

57. A method for establishing state information for a call between a calling party and a called party, comprising:

receiving, at an originating gate controller, a setup request for a call, the originating gate controller being connected to a first~~trusted~~ network, the calling party being associated with an originating interface unit coupled to a second~~an untrusted~~ network that is different from said first~~trusted~~ network;

authorizing the setup request for the call;

sending the authorized setup request to the called party;

formatting state information for the call based on a setup acknowledgment message received from the called party; and

11 sending the state information for the call from the originating gate controller to the
 12 originating interface unit;
 13 said originating gate controller and said originating interface unit communicating with
 14 one another via ~~ana-telecommunications~~ access network.

1 58. The method of claim 57, wherein the state information for the call is sent from the
 2 originating gate controller to the originating interface unit without the state information for the
 3 call being accessed subsequently from the originating gate controller.

1 59. The method of claim 58 wherein

1 60. The method of claim 59 wherein

1 61. A method for use in an originating gate controller in a packet-carrying network,
 2 the method comprising
 3 receiving a setup request for a call from an originating ~~end-terminal~~ interface unit on a
 4 ~~customer-premises~~, said setup request being received over ~~ana-telecommunications~~ access
 5 network that interconnects said ~~end-terminal~~ ~~customer-premises~~ to said packet-carrying network;
 6 and
 7 sending state information for the call to the originating ~~end-terminal~~ interface unit over
 8 said ~~telecommunications~~-access network without maintaining the state information at the
 9 originating gate controller.

1 62. The invention of claim 61 wherein said state information for the call includes
 2 information identifying a destination for the call.

1 63. The invention of claim 61 wherein said state information for the call includes
 2 billing information for the call.

1 64. The method of claim 61 wherein said state information for the call is sent to the
 2 originating interface unit in encrypted form.

65. A method for use by a gate controller in a packet-carrying network, the method comprising

receiving, from an originating ~~end-terminal~~~~interface unit on a customer premises~~, call request messages requesting setup of calls through the network, each of said call request messages including information identifying a destination for a respective one of the calls, and

sending at least one message to said originating ~~end-terminal~~~~interface unit~~ subsequent to receipt of each said call request message, ones of the sent messages including network addresses corresponding to the identified destinations and others of the sent messages including network addresses corresponding to call-forwarded destinations associated with the identified destinations,

said gate controller not maintaining information about said network addresses after sending said messages to said originating ~~end-terminal~~~~interface unit~~, and the network addresses corresponding to at least the call-forwarded destinations being encrypted.

each said message being communicated over ~~ana telecommunications~~ access network that interconnects said ~~originating end-terminal~~~~customer premises~~ with said packet-carrying network.

66. The invention of claim 65 wherein the network addresses corresponding to the identified destinations are encrypted.

67. The invention of claim 65 wherein said others of said sent messages are call transfer messages.

68. A method for use by a gate controller in a packet-carrying network of a type in which originating ~~end-terminals~~~~interface units on customer premises~~ send to said gate controller call setup requests that include information identifying requested destinations for the respective calls; said packet-carrying network further being of a type in which, subsequent to receipt of each call setup request from an individual one of the originating ~~end-terminals~~~~interface units~~, said gate controller sends to that originating ~~end-terminal~~~~interface unit~~ at least one message that includes a network address; and said packet-carrying network further being of a type in which said originating ~~end-terminals~~~~interface units~~ provide, for transport over said network, packets that include network addresses included in said messages, the method comprising

including in individual ones of the messages sent by said gate controller network addresses corresponding to said requested destinations, and including in other ones of the messages sent by said gate controller network addresses corresponding to call-forwarded destinations that had been specified for ones of said requested destinations, said gate controller not maintaining information about said network addresses after sending said messages to said originating ~~end-terminals~~~~interface units~~, and the network addresses corresponding to at least the call-forwarded destinations being encrypted, each said message being communicated over ~~ana telecommunications~~ access network that interconnects said ~~originating end-terminal~~~~customer premises~~ with said packet-carrying network.

69. The invention of claim 68 wherein said other ones of said messages are call transfer messages, whereby a call that was set up to a requested destination is caused to be transferred to a call-forwarded destination.

70. The invention of claim 68 wherein the network addresses corresponding to the identified destinations are encrypted.

71. The invention of claim 70 wherein said other ones of said messages are call transfer messages.

72. A method for use in a terminating gate controller in a packet-carrying network, the method comprising
receiving, from within said packet-carrying network, a setup request for a call, and
sending state information for the call from the terminating gate controller to a terminating end-terminal over an access network that interconnects said terminating end-terminal to said packet-carrying network without maintaining the state information at the terminating gate controller.

73. The invention of claim 72 wherein said state information for the call includes information identifying a destination for the call.

1 74. The invention of claim 72 wherein said state information for the call includes
2 billing information for the call.

1 75. The method of claim 72 wherein said state information for the call is sent to the
2 originating interface unit in encrypted form.